REMARKS

Claims 1-6 are currently pending in the subject application and are presently under consideration. Election is made to Group 1 (*e.g.*, Claims 1 and 4) and thus Claims 2, 3, 5 and 6 are withdrawn from consideration. Further, Claims 1 and 4 have been amended as shown on pp. 2-6 of the Reply. Moreover, new Claims 7-24 have been added as shown on pp. 2-6 of the Reply.

Applicants' representative thanks the Examiner for providing the telephonic interview held 26 February 2008 at 3 pm EST. Applicants' representative appreciates the Examiner indicating that the amendments to Claim 1 will be viewed favorably and that the Examiner is in agreement that Claim 1 is patentably distinct from the cited art. Applicants' representative further invites the Examiner to withdraw the restriction requirement in view of the discussion of the incorporation of novel unpacking of packed files for returning a *corresponding* unpacked executable as claimed in Claim 1 and 4. Finally, Applicants' representative thanks the Examiner for conducting the interview in light of receiving only 4 of the 8 faxed pages of the interview agenda.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1 and 4 Under 35 U.S.C. §102(e)

Claims 1 and 4 stand rejected under 35 U.S.C. §102(e) as being anticipated by Lucas *et al.*, (US 6,968,461) (hereinafter "Lucas"). Applicants' representative respectfully traverses the rejection of claims 1 and 4 under 35 USC § 102(e) as being unpatentable over Lucas.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "***each and every element*** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)) (emphasis added).

Applicants' disclosed subject matter relates to detecting malware. The malware evaluator intercepts incoming code/data and searches for malicious code. This can be done by searching

the arriving code/data for recognized patterns representative of known malicious code/data. Whereas hackers and the like have come to understand that these searches look for known patterns, the hackers have developed methods of packing malicious executable code to disguise it from traditional virus detecting software. By detecting and unpacking packed code as it arrives, *e.g.*, intercepting it, the Applicants' invention can maintain the advantage over hackers attempts at propagating malware through packed malicious executables.

The invention of Lucas generally relates to searching code for viruses in an "on-access antivirus system" (*see* Lucas, col. 3, line 47). Lucas describes that hackers have determined a particular weakness in anti-virus software that can cause the anti-virus software to "timeout" when system resources become severely taxed (*see* Lucas, col.1, ln. 11-36). Lucas proposes a solution of decompressing compressed files from a hard drive device (Lucas, col. 3, ln. 51-52) on-access and scanning these decompressed files for viruses. In Lucas's proposal, malicious files that have been compressed, so as to bog down a system on decompression, can be parsed into smaller decompressed pieces to allow for sequential scanning of each decompressed piece for virus signatures by comparison to DATs (Lucas, col. 4, ln. 7-17). Lucas does not discuss intercepting code/data as it arrives at a computer. Lucas further explicitly teaches away from unpacking large files for analysis, instead teaching that as files grow larger, they can be parsed.

With regard to Claim 1, Applicants' representative disagrees with the Examiner's position for at least the following reasons. In particular, independent claim 1 recites, "...a malware evaluator for determining whether incoming data is malware, wherein the incoming data directed to a computing device **is intercepted by the malware evaluator**..." (emphasis added). Contrary to assertions made in the Office Action, the cited reference does not disclose or suggest this feature of Applicants' claimed invention. The Applicants' invention explicitly describes intercepting incoming data wherein the invention, "operates on incoming data **as it physically arrives at the computer**...the incoming data does not actually "reach" the computer until it gets past the anti-virus software." (pg. 2, ln, 2-5, emphasis added). Applicants' further state, "the malware evaluator 308 **intercepts** the packed executable 302 **before it reaches the computer** 110...the malware evaluator 308 may **intercept** the packed executable 302 as it is routed to the computer **over a network**...may also operate to **intercept** the packed executable 302 when encountered on **distributable media**...such as a floppy disk, a flash memory...a CD-ROM disk, magnetic tape, and the like." (pg. 7, ln. 3-9, emphasis added). In contrast Lucas does

not teach intercepting malicious code before it reaches a computer, rather teaching scanning files already on a computer at the hard disk drive (*see* Lucas, col. 3, ln. 51-52). Further, Lucas explicitly illustrates the system with the hard disk drive in Figure 1 (*see* Lucas Fig. 1, HDD 10).

Additionally, Applicants' invention discloses unpacking packed executables for malware detection. Applicants' invention contemplates unpacking entire packed executables, without executing the unpacking code included in a potentially malicious packed executable, to create *corresponding* unpacked executables for analysis. This claimed feature should not be overlooked. Generally, the analysis for malware is not conducted on an actual unpacked potentially malicious piece of code or data, but rather is conducted on a representation of what the unpacked code/data would look like, but the representation is actually unpacked by a controlled unpacker (*e.g.*, by selectable unpacker modules within the unpacking module) designed to unpack specific file types. This serves to prevent execution of and infection by unpacking of the actual potentially malicious packed executable. This is explicitly claimed in Claim 1, "...receives a packed executable from the malware evaluator and returns an unpacked executable **corresponding** to the packed executable..." (emphasis added). Lucas neither explicitly nor implicitly discloses this feature of the claimed invention.

The Examiner has rejected Claim 4 based on similar reasoning as applied to Claim 1, Applicants' representative therefore similarly disagrees with the Examiner's position. In particular, independent claim 1 recites, "...**intercepting incoming data** directed to a computing device" (emphasis added). Contrary to assertions made in the Office Action, the cited reference, for the reasons disclosed herein above with respect to Claim 1, does not disclose or suggest this feature of Applicants' claimed invention. Further, Claim 4 states, "...the unpacked executable **corresponding** to the packed executable" (emphasis added). Contrary to assertions made in the Office Action, the cited reference, for the reasons disclosed herein above with respect to Claim 1, does not disclose or suggest this feature of Applicants' claimed invention.

Therefore, based on the above remarks, the Applicants respectfully request that the Examiner withdraw the rejection of Claims 1 and 4 under 35 USC § 102(e) as being anticipated by Lucas.

II. Addition of New Claims 7-24

Claims 7-24 have been added to claim aspects of the present invention illustrated in the Applicants' disclosure. Applicants' representative asserts that these claims are fully supported by the application as filed. Applicants' representative further asserts that these claims are patentably distinct over Lucas. For example, Claims 7 and 8 recite features of unpackers employed in returning a corresponding executable; Claims 9 and 10 recite features of intercepting data/code before it reaches the computer; Claims 13 and 15-17 recite features of determining malware with regard to code/data that is not a packed executable; and Claims 19-24 recite features of methods including corresponding executable aspects, aspects of intercepting code/data from networks and distributable media, and aspects of unpacking entire executables, among others. None of these features are explicitly or implicitly disclosed by Lucas.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP2193US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731